CLAIMS

What is claimed is:

1. A secure recording medium having at least one of audio, video and software content, comprising a plurality of media recording disks (DVD's) with a disk security chip embedded in each said DVD, each said disk chip comprising a security key, wherein at least two of said DVD's have different disk security keys.

2. The secure recording medium according to claim 1 and wherein said at least two of said DVD's have common content recorded therein.

3. The secure recording medium according to claim 1 or claim 2 and wherein said medium has audio content and video content and said security key is different for audio content than for video content.

4. The secure recording medium according to any of claims 1-3 and comprising a first antenna disposed in said DVD which is in electrical communication with said disk security chip.

5. The secure recording medium according to any of claims 1-4 and wherein said DVD is substantially statically balanced.

6. The secure recording medium according to any of claims 1-5 and wherein said DVD is substantially dynamically balanced.

7. The secure recording medium according to any of claims 4-6 and further comprising a DVD player, said player comprising a second antenna which is in wireless communication with said first antenna.

8. The secure recording medium according to claim 7 and further comprising a player security chip in electrical communication with said second antenna.

9. The secure recording medium according to claim 8 and wherein said player security chip decrypts data received from said disk security chip.

10. The secure recording medium according to claim 8 or claim 9 and wherein said player security chip is integrated into a circuit of an integrated receiver decoder of said DVD player.

11. The secure recording medium according to any of claims 8-10 and wherein said player security chip is detachable from said DVD player.

12. The secure recording medium according to any of claims 8-11 and wherein said player security chip is generally tamper-resistant.

13. The secure recording medium according to any of claims 8-12 and wherein said player security chip is generally clone-resistant.

14. The secure recording medium according to any of claims 8-13 and wherein said player security chip is upgradable.

15. The secure recording medium according to any of claims 8-14 and wherein said player security chip is backwardly compatible with a previous version of at least one of said player security chip and said disk security chip.

16. The secure recording medium according to any of claims 8-15 and wherein said player security chip performs an authentication process with said disk security chip.

17. The secure recording medium according to claim 16 and wherein said player security chip verifies legitimacy of said disk security chip by means of a function of a geometric property of said DVD.

18. The secure recording medium according to claim 17 and wherein said function is selected from the group consisting of a function of an angle between layers of said DVD, a diameter of said DVD, a thickness of said DVD and an eccentricity of said DVD.

19. The secure recording medium according to any of claims 8-18 and wherein said disk security chip performs an authentication process with said player security chip.

20. The secure recording medium according to claim 19 and wherein said authentication process comprises a mutual zero-knowledge interaction authentication process.

21. A secure recording medium comprising a media recording disk (DVD) with a disk security chip embedded therein, characterized by said DVD being substantially statically balanced.

22. The secure recording medium according to claim 21 wherein said DVD is substantially dynamically balanced.

23. A secure recording medium comprising:

a media recording disk (DVD) with a disk security chip embedded therein;

a first antenna disposed in said DVD which is in electrical communication with said disk security chip; and

a DVD player, said player comprising a second antenna which is in wireless communication with said first antenna;

characterized in that said secure recording medium further comprises a player security chip in electrical communication with said second antenna.

24. The secure recording medium according to claim 23 and wherein said player security chip decrypts data received from said disk security chip.

25. The secure recording medium according to claim 23 or claim 24 and wherein said player security chip is integrated into a circuit of an integrated receiver decoder of said DVD player.

26. The secure recording medium according to any of claims 23-25 and wherein said player security chip is detachable from said DVD player.

27. The secure recording medium according to any of claims 23-26 and wherein said player security chip is generally tamper-resistant.

28. The secure recording medium according to any of claims 23-27 and wherein said player security chip is generally clone-resistant.

29. The secure recording medium according to any of claims 23-28 and wherein said player security chip is upgradable.

30. The secure recording medium according to any of claims 23-29 and wherein said player security chip is backwardly compatible with a previous version of at least one of said player security chip and said disk security chip.

31. The secure recording medium according to any of claims 23-30 and wherein said player security chip performs an authentication process with said disk security chip.

32. A secure recording medium comprising:

a media recording disk (DVD) with a disk security chip embedded therein;

a first antenna disposed in said DVD which is in electrical communication with said disk security chip;

a DVD player, said player comprising a second antenna which is in wireless communication with said first antenna; and

a player security chip in electrical communication with said second antenna,

characterized by said player security chip verifying legitimacy of said disk security chip by means of a function of a geometric property of said DVD.

33. The secure recording medium according to claim 32 and wherein said function is selected from the group consisting of a function of an angle between layers of said DVD, a diameter of said DVD and a thickness of said DVD.

34. A secure recording medium comprising:

a media recording disk (DVD) with a disk security chip embedded therein;

a first antenna disposed in said DVD which is in electrical communication with said disk security chip;

a DVD player, said player comprising a second antenna which is in wireless communication with said first antenna; and

a player security chip in electrical communication with said second antenna,

characterized by an authentication process being performed between said player security chip and said disk security chip.

35. The secure recording medium according to claim 34 wherein said authentication process comprises a mutual zero-knowledge interaction authentication process.

36. A method for protecting access to content recorded on a media recording disk (DVD), comprising:

providing a disk security chip on the DVD, said disk security chip managing access to the content of the DVD;

providing a corresponding player security chip in a DVD player which is operative to play the DVD, said player security chip managing use of a data stream

received from the DVD, said disk security chip being in wireless communication with said player security chip; and

providing said disk security chip with a disk key not known to a disk manufacturer.

37. A method for protecting access to content recorded on a media recording disk (DVD), comprising:

providing a disk security chip on the DVD, said disk security chip managing access to the content of the DVD;

providing a corresponding player security chip in a DVD player which is operative to play the DVD, said player security chip managing use of a data stream received from the DVD, said disk security chip being in wireless communication with said player security chip; and

providing a player key common to a plurality of said DVD players during a predetermined period of time.

38. The method according to claim 36 or claim 37 and comprising encrypting contents of said DVD with a content key.

39. The method according to any of claims 36-38 and comprising performing an authentication process between said disk security chip and said player security chip.

40. The method according to claim 39 and wherein said authentication process comprises a mutual zero-knowledge interaction authentication process.

41. The method according to any of claims 36-40 and wherein said disk security chip, after assuring that said DVD player is authentic, sends said DVD player said disk key.

42. The method according to any of claims 36-40 and wherein said disk security chip, after assuring that said DVD player is authentic, sends said DVD player said disk key encrypted with said player key.

43. The method according to any of claims 36-42 and wherein said player security chip verifies legitimacy of said disk key as a function of a geometric property of said DVD.

44. The method according to claim 43 and wherein said DVD is a multi-layer DVD and said geometric property is an angle between layers of said DVD.

45. The method according to any of claims 36-44 and further comprising:

said player security chip sending a random number R to said disk security chip, said random number R being different each time said DVD is played;

said disk security chip sending said player security chip an encrypted concatenation of a hash function of R, called h(R), and said content key, encrypted with said disk key;

said player security chip decrypting said concatenation, and computing h(R) and comparing with the h(R) sent by the disk security chip;

said player security chip verifying R to be correct, thereby certifying that said disk chip really knows said player key;

said player security chip obtaining content key from said concatenation; and

said player security chip using said content key to decrypt control words that are located within ECM's in said DVD.

46. A method for protecting access to content recorded on a media recording disk (DVD), comprising:

providing a disk security chip on the DVD, said disk security chip managing access to the content of the DVD;

providing a corresponding player security chip in a DVD player which is operative to play the DVD, said player security chip managing use of a data stream received from the DVD, said disk security chip being in wireless communication with said player security chip; and

performing an authentication process between said disk security chip and said player security chip.

47. The method according to claim 46 and wherein said authentication process comprises a mutual zero-knowledge interaction authentication process.

48. A method for protecting access to content recorded on a media recording disk (DVD), comprising:

providing a disk security chip on the DVD, said disk security chip managing access to the content of the DVD;

providing a corresponding player security chip in a DVD player which is operative to play the DVD, said player security chip managing use of a data stream received from the DVD; and

communicating information from said player security chip to said disk security chip by illuminating selected tracks on said DVD that are covered with photo-sensitive materials, whereby said disk security chip monitors the illuminated tracks. that are illuminated by the laser head.

49. The method according to claim 48 and further comprising communicating information from said disk security chip by covering said laser-head illumination tracks on said DVD with a voltage-controlled semi-opaque material, and then using said disk security chip to control opacity of the semi-opaque material by appropriately controlling a voltage thereat, the degree of opacity being used to communicate the information from said disk security chip to said player security chip.

50. A method for protecting access to content recorded on a media recording disk (DVD), comprising:

providing a DVD with content recorded thereon which is to be protected;

providing a disk security chip on a media recording disk different from the DVD, said disk security chip managing access to the content of the DVD; and

providing a corresponding player security chip in a DVD player which is operative to play the DVD, said player security chip managing use of a data stream received from the DVD, said disk security chip being in wireless communication with said player security chip.

51. A secure recording medium having at least one of audio, video and software content, comprising a stiffy disk with a disk security chip embedded thereon, said disk chip comprising a security key.

Add A17